UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/720,329	11/24/2003	Weng-Chin Yung	079171.0160	4304

5073 7590 01/23/2009

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
MILLS, DONALD L	
ART UNIT	**PAPER NUMBER**
2416	

NOTIFICATION DATE	DELIVERY MODE
01/23/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary	**Application No.** 10/720,329	**Applicant(s)** YUNG ET AL.	
	Examiner DONALD L. MILLS	**Art Unit** 2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21 and 23-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21 and 23-33* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-20 and 26-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-20 and 26-33 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The facilitating classification of data flows method including steps of monitoring, comparing, and classifying, and is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. For example, referring to claim 1, the claim does not specify a machine or apparatus to facilitate the performance of the classification.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 2, 8-10, 12-16, 20 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Packer (US 6,046,980).

Regarding claim 1, Packer discloses in Fig 1 D, a TCP/IP suite that facilitate classification of data flows comprising monitoring a data flow associated with a host relative to at least one behavioral attribute [monitor network status parameters, see col. 9, lines 19-20]; comparing the least one behavioral attribute observed in the monitoring step to a knowledge base of at least one know application behavior pattern, wherein the at least one known application behavior pattern corresponds to a network application classification and comprises one or more behavioral attribute parameter values [checks each level of the classification tree, matches the attributes of a given traffic class if the flow being classified matches attributes of a given traffic class, see col. 11, lines 55-58 and Fig. 3; classifier 304]; and classifying the data flow into a network application classification based on the comparing step [the class at the level that matches determines the policy for the flow being classified, see col. 11, lines 62-63].

Regarding claim 2, Packer discloses a method wherein at least one behavioral attribute is packet size of the first packet in the data flow [see col. 12, Table 2, IP address includes the packet size].

Regarding claim 8, Packer discloses a method wherein at least one behavioral attribute is the timing of the data flow relative to at least one similar data flow associated with the host [determining a data link rate and latency period from an exchange of packet(s) between TCP endpoints, see Fig. 1E; where Tdatal is the arrival time of first data packet and Tbase is the reference time, see col. 10, lines 32-42].

Regarding claim 9, Packer discloses a method wherein at least one behavioral attribute is the number of related data flows associated with the host [The initial data packets are examined as they establish a connection. Parameters are developed from which RTT and Max data rate can be determined, see col. 10, lines 22-24].

Regarding claim 10, Packer discloses a method wherein at least one behavioral attribute is the timing between at least two packets in the data flow [determining a data link rate and latency period from an exchange of packet(s) between TCP endpoints, see Fig. 1E; where Tdatal is the arrival time of first data packet and Tbase is the reference time, see col. 10, lines 32-42].

Regarding claims 12 and 13, Packer discloses a method wherein at least one behavioral attribute is timing and sequence of protocol flags contained in packets of the data flow [The SYN packets takes a finite but unknown transit time to arrive at the local TCP endpoint, where the local TCP endpoint responds with its own SYN packet (packet is of known length, issued at a know time, see col. 10, lines 37.40 and Fig. 1E; HTTP request from server to client].

Regarding claim 14, Packer discloses a method wherein the application behavior pattern comprises at least one instance of any one of the following: packet size pattern [see col. 12, Table 2, IP address includes the packet size], a threshold information density value, a threshold inter-flow timing value [values are obtained for serialization of n, the size of the SYN packet in response and the size of the ACK packet, see col. 10, lines 61-63], or a threshold number of related application data flows [TCP autobaud component 302 determines values for selectable information such as flow data rate, see col. 15, lines 24-25].

Regarding claim 15, Packer discloses a method wherein the application behavior pattern characterizes the first group of packets of a data flow associated with a traffic class [a traffic specification of a child node, such as FTP node 206 is compared with a flow specification of the new flow 300, if a match is discovered the processing in flowchart 511 is applied to the child node recursively (same traffic class), see col. 18, lines 9-13. If no policy exists, processing backtracks to a parent node and looks for a policy associated with the parent node to apply to the new flow, see col. 18, lines 21-23].

Regarding claim 16, Packer discloses a method wherein the application behavior pattern characterizes the first group of packets of a data flow associated with a traffic class Jail traffic which does not match any user specified traffic class falls into an automatically created default traffic class, which has a default policy, see col. 12, lines 66-68] and wherein the first group of packets are characterized in relation to at least one instance of any one of the following: a packet size pattern [web traffic may have a service level defined for html (small files) and a separate traffic class for gif files (reserved service for larger files), see col. 13, lines30-33], a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows [determining an acceptable allocation of bandwidth to reserved service flows, i.e., GIR or EIR, by allocating rate for each gear 410 or 411, based upon individual flow demands, base limits and total limits, see col. 18, lines 29-33].

Regarding claim 20, Packer discloses a method wherein monitoring the data flows associated with a host relative to at least one application behavior model corresponding to a traffic class [bandwidth resource needs of multiple requesting flows are reconciled in accordance with policy of each flow based upon the flow's class, see col. 4, lines 10-12]; matching at least one of the data flows associated with the host to a traffic class if a threshold number of the data flows match a corresponding application behavior model; wherein the application behavior model comprises at least one instance of any one of the following: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet timing value, a sequence of protocol flags, an inter-packet protocol flag timing value [available bandwidth may be allocated among flows, according to policy (and by priority) which may include any combination of GIR or EIR and the flows are limited to a total number functionally equivalent to a threshold, see col. 4, lines 5-8].

Regarding claim 26, Packer teaches of a method comprising detecting a data flow in network traffic traversing a communications path, the data flows each comprising at least one packet [Fig 1B; initiating a new flow between client and server with data objects sent to and from the network]; parsing explicit attributes at least one packet associated with the data flow into a flow specification [a bandwidth manager 306 uses the policy determined by classifier 304 1 n order to allocate bandwidth according to the service level prescribed by the policy, see col. 15, lines 33-35], matching the flow specification to a first plurality of traffic classes, wherein the first plurality of traffic classes are each defined by one or more matching attributes [Fig 2A and 2B; data flow assigned to TCP data flow specification, with other matching attributes such as bandwidth allocation for FTP or Web files], having found a matching traffic class in the matching step, associating the flow specification corresponding to the data flow with a traffic class from the first plurality of traffic classes [see Fig 2E and 5F, where data flow is assigned to the a specification tree and subsequently assigned to root policy or a recursive child policy in the tree], not having found a matching traffic class in the first plurality of traffic classes matching the data flow to at least one additional traffic class, the additional traffic class defined by an application behavior pattern [all traffic which does not match any user specified traffic class falls into an automatically created default traffic class, which has a default policy, see col. 12, lines 66-68], the application behavior pattern comprising comprises at least one instance of: a packet size pattern [web traffic may have a service level defined for html (small files) and a separate traffic class for gif files (reserved service for larger files), see col. 13, lines30-33], a threshold information density value, a threshold inter-flow timing value [values are obtained for serialization of n, the size of the SYN packet in response and the size of the ACK packet, see col. 10, lines 61-63], or a threshold number of related application data flows [determining an acceptable allocation of bandwidth to reserved service flows, i.e., GIR or EIR, by allocating rate for each gear 410 or 411, based upon individual flow demands, base limits and total limits, see col. 18, lines 29-33].

5. Claim 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Aimoto et al. (US 6,144,636), hereinafter referred to as Aimoto.

Regarding claim 17, Aimoto discloses in the abstract, a method wherein modeling the behavior of a network application to generate an application behavior pattern corresponding to the network application [an input packet from the input port is delivered to at least one output 'port in accordance with address information of the input packet and connection information having been set (configured) at the time of setting the connection between the transmission source and destination]; and configuring a network traffic monitoring device to monitor data flows relative to at least one behavioral attribute and classify the classify data flows into a traffic class of a plurality of traffic classes by comparing one or more of the data flows against the application behavior pattern [an ABR congestion control function for a switch of shared buffer construction (classes) in which a cell buffer is shared by a plurality of ports bandwidth, see col. 18, lines 61-63, wherein the ABR traffic class, a bandwidth management cell periodically transmits predetermined number of data cells, see col. 2, lines 10-11]; wherein the application behavior pattern comprises at least one instance of any one of the following: a packet size pattern [a Constant Bit Rate traffic class in which a fixed amount of bandwidth is continuously made available by the network to transfer cells, see col. 1, lines53-55], a threshold information density value [information on a threshold value (information density) for each traffic class are held within the packet switch, see col. 3, lines 18-20], a threshold inter-flow timing value, or a threshold number of related application data flows [a table having plurality of entries which illustrates behavior of congestion notification, see col. 17, lines 46-47].

6. Claims 29-33 are rejected under 35 U.S.C. 102(b) as being anticipated by Bennett (US 6,122,670).

Regarding claim 29, Bennett discloses a method comprising detecting a data flow in network traffic traversing a communication path, the data flow comprising at least one packet [nodes interconnected to form several hosts of WAN/LAN networks (Fig.l) where discoverable protocol is know to be TCP based on the application and FTP sewer (Fig.2)]; classifying the data flow into a network application of a plurality of network applications by applying a mathematical function to at least one packet in the data flow to derive a computer value that characterizes entropy of information contained in the at least one packet, wherein the entropy information corresponds to a level of randomness of data of the at least one packet [IP header checksum - hardware calculation - performed on receive packet to reassemble IP datagram or datagram fragment to its original structure, functionally equivalent to a classification, col. 6, lines 28-30 and Fig 6]; comparing the computed value to at least one traffic class corresponding to the network application, said traffic class defined, at least in part, by a required computed entropy value [protocol logic subsystem verifies traffic class; IP header and TCP segment checksums before sending datagram col. 6, lines 34-37].

Regarding claim 30, Bennett discloses a method wherein the required computed value is determined by applying the mathematical function to data flows know to be Of the traffic class [the header check sum is indicated by the fragment bit flag 301 and offset fragment 302 which ensures datagram validity. Based on fragment bits set, the datagram is stored in memory based on its relative offset from the beginning of the original datagram or in its own base address in memory, see col. 8, lines 34-43].

Regarding claim 31, Bennett discloses a method wherein the mathematical function computes a value indicating the information density of at least one packet [based on relative offsets and partial checksums calculated, other datagrams that are received with identical identification filed 333, source and destination IP addresses, they are known to be another following fragment of a first fragment, see col. 7, lines 45-50].

Regarding claim 32, Bennett discloses a method wherein the required computed value is a range of values [the reconfigurable protocol logic has memory recourses for datagram storage, and lookup tables for datagram de-fragmentation and other protocol functions, see col. 11, lines 10-15].

Regarding claim 33, Bennett discloses a method comprising detecting a data flow in network traffic traversing a communication path, the data flow comprising at least one packet containing a first checksum [nodes interconnected to form several hosts of WANILAN networks (Fig.l) where discoverable protocol is know to be TCP based on the application and FTP server (Fig.2)]; applying a mathematical function to at least one packet in the data flow to derive a second checksum [IP header checksum - performed on receive packet to reassemble IP datagram or datagram fragment to its original structure, col. 6, lines 28-30 and Fig 6]; comparing the computed second checksum to the first checksum value contained in at least on packet [protocol logic subsystem verifies traffic class; IP header and TCP segment checksums before sending datagram col. 6, lines 34-37]; matching the data flow to a traffic class, wherein the traffic class is defined at least in part by whether the computed second checksum should match the first checksum in the at least one packet [based on relative offsets and partial checksums (TCP/UDP protocol) calculated, other datagrams that are received with identical identification filed 333, source and destination IP addresses, are known to be another following fragment of a first fragment and subsequently added, see col. 7, lines 45-50].

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Packer (US 6,046,980) in view of Bennett (US 6,122,670).

Regarding claims 3 and 4 as explained in the rejection statement of claim 1, Parker discloses all of the claim limitations of claim 1 (parent claim).

Parker does not disclose of a method wherein at least one behavioral attribute is packet size of the first packet in the data flow.

However, Bennett teaches of a method where [a memory 40 in a network card 2000, stores command lists for disposition queue of datagrams, see col. 6, lines 11-13. When a packet is received, network interface 50 reassembles the IP datagram or datagram fragments and then writes the corresponding datagram fragments to datagram buffer 53, see col. 6, lines 27-30. Where flag 301 and fragment offset 302 together indicate whether datagram 332 is a fragment of a larger datagram, see col. 6, lines 65-67].

Based on the teachings of Bennett, at the time of the invention, it would have been obvious to a person in ordinary skill in the art to incorporate the network card of Bennett in a traffic class at any level of the TCP/IP protocol or (traffic classification tree in Fig. 2C), whereby configuring a traffic class node that would specify policies by using the flag 301 and fragment offset 302 as taught by Bennett to classify dataflow according to n-array, i.e. first, second ... ,nth datagram or datagram fragments, see col. 14, lines, Fig. 2C and Fig. 2D. Thus, it would have been obvious to one of ordinary skill in the art a the time to be motivated to incorporate the IP flag together with a fragment offset as one behavioral attribute to provide the ability to classify and search traffic based upon multiple orthogonal classification attributes.

Regarding claim 5 as explained in the rejection statement of claim 1, Parker discloses all of the claim limitations of claim 1 (parent claim).

Packer does not disclose of a method wherein at least one behavioral attribute is packet size of plurality of packets in the data flow.

However, Bennett teaches of a method where [an IP datagram identifier are checked against any other recently received datagrams by a de- fragmentation lookup subsystem. Either a new allocation in datagram memory 53 is created for new IP datagram identifiers, or datagram fragments are stored (accumulated) with other fragments from the same IP datagram identifier by returning the base address of the memory allocation in 53 where the previously received fragment(s) where stored, see col. 13, lines 18-24. The Protocol logic 45 sums the data (IP and TCP checksums) and transfers these sums to the accumulation register, see lines 46-48].

Based on the teachings of Bennett, at the time of the invention, it would have been obvious to a person in ordinary skill in the art to incorporate the network card of Bennett in a traffic class at any level of the TCP/IP protocol or (traffic classification tree in Fig. 2C), whereby configuring a traffic class node that would specify policies by using the end of the IP header of Bennett, as indication of the amount of data having been transferred equaling the value in header length field or (packet size). Thus, it would have been obvious to one of ordinary skill in the art a the time to be motivated to incorporate the header length as one behavioral attribute to provide the ability to classify and search traffic based upon multiple orthogonal classification attributes.

9. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Packer (US 6,046,980) in view of Aimoto (US 6,144,636).

Regarding claim 6 as explained in the rejection statement of claim 1, Packer discloses all of the claim limitations of claim 1 (parent claim).

Packer does not disclose a method wherein at least one behavioral attribute is the information density associated with at least one packet in the data flow, wherein the information density corresponds to a level of randomness of data of the at least one packet.

Aimoto teaches a technique wherein information on a counter and information on a threshold value (information density corresponding to a level of randomness) for each traffic class are held within the packet switch, see col. 3, lines 18-20.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the packet switch and congestion notification method of Aimoto in the system of Packer. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system for managing flow bandwidth which recognized the congestion state of the packet switch to improve system efficiency and quality, as taught by Aimoto (See Abstract.)

Regarding claim 7 as explained in the rejection statement of claim 1, Packer discloses all of the claim limitations of claim 1 (parent claim).

Packer does not disclose a method wherein at least one behavioral attribute is the information density, wherein the information density corresponds to a level of randomness of data of the at least one packet.

Aimoto teaches information on a counter and information on a threshold value (information density corresponding to a level of randomness) for each traffic class are held within the packet switch, see col. 3, lines 18-20, associated with the first packet in the data flow (buffers such as RIRO type input buffers and FIFO type out put buffers are included in the packet switch and an input buffer control unit determines a cell which is to be delivered, see col. 2, lines 38-41).

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the packet switch and congestion notification method of Aimoto in the system of Packer. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system for managing flow bandwidth which recognized the congestion state of the packet switch to improve system efficiency and quality, as taught by Aimoto (See Abstract.)

10. Claims 11, 27, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Packer (US 6,046,980) in view of Bennett (US 6,122,670).

Regarding claim 11 as explained in the rejection statement of claim 1, Packer discloses all of the claim limitations of claim 1 (parent claim).

Packer does not disclose a method wherein at least one behavioral attribute is a sequence of protocol flags contained in packets of the data flow.

Bennett teaches a reconfigurable protocol logic subsystem, coalesces numerous operations from the various protocols which speed up the overall system processing, see col. 3, lines 50-51 and Fig. 4, protocol logic 45.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of sending and receiving data of Bennett in the system of Packer. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system capable of recognizing TCP protocol, as taught by Bennett (See Abstract.)

Regarding claim 27 as explained in the rejection statement of claim 21, Packer discloses all of claim limitations of claim 21.

Packer does not disclose *wherein said flow specification contains at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a MIME type, and a pointer to an application specific attribute.*

Bennett teaches an apparatus wherein Flow specification contains at least one instance of any one of the following; a protocol family designation [Fig.2A; TCP or a UDP process], a direction of packet flow designation, a protocol type designation [see Fig. 18A and 18B, processing of incoming TCP segments constitutes a bi-directional flow of data between FTP server and FTP client], a protocol type designation [see Fig. 6; source IP address 306 and destination IP address 308], a pair of hosts, a pair of ports a pointer to a MIME type, and a pointer to an application-specific attribute [commands for both TCP ACK and for a disposition queue of pending datagrams; a queue of pointers to datagrams which need to be transferred to the network, see col. 6, lines 12-16].

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of sending and receiving data of Bennett in the system of Packer. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system capable of recognizing TCP protocol, as taught by Bennett (See Abstract.)

Regarding claim 28 as explained in the rejection statement of claim 21, Packer discloses all of claim limitations of claim 21.

Packer does not disclose *wherein said flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a MIME type, and a pointer to an application-specific attribute.*

Bennett teaches an apparatus wherein Flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation [Fig.2A; TCP or a UDP process], a direction of packet flow designation [see Fig. 18A and 18B, processing of incoming TCP segments constitutes a bi-directional flow of data between FTP server and FTP client], a protocol type designation, a pair of hosts [see Fig. 1; nodes interconnected to form several hosts of WAN/LAN networks], a pair of ports [see Fig. 7; source port 310 and destination port 312], a pointer to a MIME type, and a pointer to an application-specific attribute [see Fig. 6, flags 301; fragments of original datagram and fragment offset 302; indicates bytes of original datagram length 330].

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of sending and receiving data of Bennett in the system of Packer. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system capable of recognizing TCP protocol, as taught by Bennett (See Abstract.)

11. Claims 17-19 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aimoto (US 6,144,636) in view of Bennett (US 6,122,670).

Re claim 21, Aimoto discloses in Fig. 1 and abstract of the prior art, an apparatus wherein a packet processor (switch 100) operative to detect data flows in network traffic traversing a communication path [communication is transferred from terminal A toward terminal B via the switch, col. 9, lines 2-26], the data flows each comprising at least one packet (header conversion circuit 132 and line input controller133); parse at least one packet associated with a data flow into a flow specification [input packet is delivered to at least one output port in accordance with address information of the input packet and connection info set in the packet switch at the time of connection setup], a traffic classification engine operative to match the data flow to a plurality of traffic classes, at least one of the traffic classes defined by one or more application behavior patterns [the marking mode provides at least the following apparatus in the switch for the congestion decision/notification circuit; cell number counter information, threshold value for every connection a comparator unit is also provided for every connection, connection number count, target bandwidth information register, etc. See col. 6, lines 38-46]; having found a matching traffic class in the matching step [the results of the comparator circuit in Fig. 5 is provided for every connection for deciding whether the value of a cell number counter has exceeded a threshold value information of all output ports held in the switch, see col. 6, lines 6-8], associate the flow specification corresponding to the data flow with a traffic class from the plurality of traffic classes [the bandwidth management cell which contains congestion notifications (max. bandwidth for a transmission) inserted by the decision/notification circuit decides whether the congestion notification of every connection is to performed in compliance with notification of the congested state for all output ports or, whether the congestion notification is to be immediately performed, see col. 6, lines 31-35] At least one of the plurality of traffic classes is defined by one or more matching attributes [the marking mode provides at least the following apparatus in the switch for the congestion decision/notification circuit; cell number counter information, threshold value for every connection a comparator unit is also provided for every connection, connection number count, target bandwidth information register, etc. See col. 6, lines 38-46], wherein Said matching attributes are explicitly presented in the packets associated with the data flows [each congestion notification includes a binary marking mode (to include an explicit rate field, binary marking filed and a maximum rate field) in which the source terminal is notified of an allowed transmission, see col. 10, lines 10-14].

Aimoto does not disclose *wherein the application behavior patterns each comprise at least any one of the following: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet timing value, a sequence of protocol flags, or an inter-packet protocol flag timing value.*

Bennett teaches a packet size pattern [source port field 310 and destination port field 312, see Fig. 7], a threshold information density value, a threshold inter-flow timing value [a buffer with command lists for both TCP ACK commands and for disposition queues for pending datagrams, see col. 6, lines 11-13], or a threshold number of related application data flows [TCP process includes instructions for sending data to FTP client and also receiving data from FTP via buffers, see col. 4, lines 50-53 and Fig. 2B], an inter-packet timing value[Datagram ID numbers, source IP addresses are passed via means of communication to the de- fragmentation lookup subsystem, see col. 9, lines 20-23 and Fig. 9, reconfigurable FPGAs 922 and 924], a sequence of protocol flags [see Fig. 4, protocol logic device 45], an inter-packet protocol flag timing value.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of sending and receiving data of Bennett in the system of Aimoto. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system capable of recognizing TCP protocol, as taught by Bennett (See Abstract.)

Regarding claim 18 as explained in the rejection statement of claim 17, Aimoto discloses all of the claim limitations of claim 17.

Aimoto does not disclose a method wherein the application behavior pattern comprises at least one instance of any one of the following: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet value, a sequence of protocol flags, an inter-packet protocol flag timing value.

Bennett teaches a packet size pattern [source port field 310 and destination port field 312, see Fig. 7], a threshold information density value, a threshold inter-flow timing value [a buffer with command lists for both TCP ACK commands and for disposition queues for pending datagrams, see col. 6, lines 11-13], or a threshold number of related application data flows [TCP process includes instructions for sending data to FTP client and also receiving data from FTP via buffers, see col. 4, lines 50-53 and Fig. 2B], an inter-packet timing value[Datagram ID numbers, source IP addresses are passed via means of communication to the de- fragmentation lookup subsystem, see col. 9, lines 20-23 and Fig. 9, reconfigurable FPGAs 922 and 924], a sequence of protocol flags [see Fig. 4, protocol logic device 45], an inter-packet protocol flag timing value.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of sending and receiving data of Bennett in the system of Aimoto. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system capable of recognizing TCP protocol, as taught by Bennett (See Abstract.)

Regarding claim 19 as explained in the rejection statement of claim 17, Aimoto discloses all of the claim limitations of claim 17.

Aimoto does not disclose *wherein the protocol flags are TCP protocol flags.*

Bennett teaches in Fig. 1, a TCP/IP protocol stack. The protocol flags are TCP protocol flags [TCP process includes instructions for sending data to FTP client and also receiving data from FTP via buffers, see col. 4, lines 50-53 and Fig. 2B].

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of sending and receiving data of Bennett in the system of Aimoto. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system capable of recognizing TCP protocol, as taught by Bennett (See Abstract.)

Regarding claim 23 as explained in the rejection statement of claim 21, Aimoto discloses all of claim limitations of claim 21.

Aimoto does not disclose *wherein said flow specification contains at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a* *protocol type designation, a pair of hosts, a pair of ports, a pointer to a MIME type, and a pointer to an application specific attribute.*

Bennett teaches an apparatus wherein Flow specification contains at least one instance of any one of the following; a protocol family designation [Fig.2A; TCP or a UDP process], a direction of packet flow designation, a protocol type designation [see Fig. 18A and 18B, processing of incoming TCP segments constitutes a bi-directional flow of data between FTP server and FTP client], a protocol type designation [see Fig. 6; source IP address 306 and destination IP address 308], a pair of hosts, a pair of ports a pointer to a MIME type, and a pointer to an application-specific attribute [commands for both TCP ACK and for a disposition queue of pending datagrams; a queue of pointers to datagrams which need to be transferred to the network, see col. 6, lines 12-16].

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of sending and receiving data of Bennett in the system of Aimoto. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system capable of recognizing TCP protocol, as taught by Bennett (See Abstract.)

Regarding claim 24 as explained in the rejection statement of claim 21, Aimoto discloses all of claim limitations of claim 21.

Aimoto does not disclose *wherein said flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of* *hosts, a pair of ports, a pointer to a MIME type, and a pointer to an application-specific attribute.*

Bennett teaches an apparatus wherein Flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation [Fig.2A; TCP or a UDP process], a direction of packet flow designation [see Fig. 18A and 18B, processing of incoming TCP segments constitutes a bi-directional flow of data between FTP server and FTP client], a protocol type designation, a pair of hosts [see Fig. 1; nodes interconnected to form several hosts of WAN/LAN networks], a pair of ports [see Fig. 7; source port 310 and destination port 312], a pointer to a MIME type, and a pointer to an application-specific attribute [see Fig. 6, flags 301; fragments of original datagram and fragment offset 302; indicates bytes of original datagram length 330].

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of sending and receiving data of Bennett in the system of Aimoto. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to realize a system capable of recognizing TCP protocol, as taught by Bennett (See Abstract.)

Regarding claim 25, the primary reference further teaches at least one of the plurality of traffic classes is defined by one or more matching attributes [the marking mode provides at least the following apparatus in the switch for the congestion decision/notification circuit; cell number counter information, threshold value for every connection a comparator unit is also provided for every connection, connection number count, target bandwidth information register, etc. See col. 6, lines 38-46], wherein said matching attributes are explicitly presented in the packets associated with the data flows [each congestion notification includes a binary marking mode (to include an explicit rate field, binary marking filed and a maximum rate field) in which the source terminal is notified of an allowed transmission, see col. 10, lines 10-14].

Response to Arguments

12. Applicant's arguments filed 15 October 2008 have been fully considered but they are not persuasive.

On page 9 of the remarks, regarding claims 1, 20, 21, and 26, the Applicant argues the primary reference does not teach all of the claim limitations. The Examiner respectfully disagrees. Neither the original nor the amended claims reflect any structural or functional matter which would differentiate the claims from the prior art. The Applicant utilizes merely descriptive terms, such as "behavior pattern" and "behavioral attribute parameter values" that lack any structural or functional matter. The Examiner utilizes a broad literal reasonable interpretation, which teaches all of the claimed limitations. The Applicant appears to read limitations from the specification into the claims; however, claims are merely read in-light of the specification. Should the Applicant intend for an interpretation as described in the remarks and specification, the Examiner encourages the Applicant to amend the claims to reflect such an intention.

On page 11 of the remarks, regarding claims 2-5, the Applicant argues that Packer does not disclose a method wherein at least one behavioral attribute is packet size of the first packet in the data flow. The Examiner respectfully disagrees. Packer discloses a packet, comprising a size, which is used to determine an IP address (See col. 12, Table 2, IP address). Regarding claims 3-5, the Applicant argues neither Packer nor Bennett disclose, teach, or otherwise make obvious classifying data flows into "network application traffic classifications" based on behavior patterns that consider the sizes of packets of data flow. The Examiner respectfully disagrees. The Examiner interprets the claim limitations as corresponding to receiving a packet fragment and performing reassembly of the data fragments to produce a packet. In this manner, the size of the packets are considered and the process of reassembly is functionally equivalent to "classifying data flows into network application traffic classifications."

On page 12 of the remarks, regarding claims 6 and 7 (as well as, claims 29-32 as argued on page 14 of the remarks), the Applicant argues neither Packer nor Aimoto disclose, teach, or otherwise make obvious information density corresponding to a level of randomness of data of the at least one packet. Again, the Applicant utilizes merely descriptive terms, which lack any structural or functional matter. The Examiner utilizes a broad literal reasonable interpretation, which teaches all of the claimed limitations. More specifically, Aimoto teaches a technique wherein information on a counter and information on a threshold value (information density corresponding to a level of randomness) for each traffic class are held within the packet switch (see col. 3, lines 18-20). The claim limitation merely states "information density corresponding to a level of randomness of data of the at least one packet"; therefore, if the randomness is non-existent the limitation bears little weight.

On page 12 of the remarks, regarding claims 8 and 9, the Applicant argues Packer does not disclose a traffic classification system that uses a behavior pattern that considers the presence of other, similar data flows associated with the same host. The Examiner respectfully disagrees.

The claim does not specify "data flows associated with the same host," the claim merely specifies the host. Therefore, the Examiner's interpretation and rejection is substantially correct.

On page 13 of the remarks, regarding claims 10-16, the Applicant argues Packer does not disclose a method wherein at least one behavioral attribute is the timing between at least two packets in the data flow. The Examiner respectfully disagrees. Packer determines a data link rate and latency period from an exchange of packet(s) between TCP endpoints, see Fig. 1E; where Tdatal is the arrival time of first data packet and Tbase is the reference time (see col. 10, lines 32-42). Regarding claim 11, the Applicant argues Bennett does not teach a method wherein at least one behavioral attribute is a sequence of protocol flags contained in packets of the data flow. The Examiner respectfully disagrees. Bennett teaches a reconfigurable protocol logic subsystem, which coalesces numerous operations from the various protocols which speed up the overall system processing (see col. 3, lines 50-51 and Fig. 4, protocol logic 45).

On page 14 of the remarks, regarding claim 17, the Applicant argues Aimoto is directed to network switch with congestion control function but does not actually classify traffic classes. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

On page 15 of the remarks, regarding claim 33, the Applicant argues Bennett does not disclose classification of data flows based on behavior patterns that consider whether the computed second checksum should match the checksum contained in received packets. The Examiner respectfully disagrees. Bennett discloses Bennett discloses matching the data flow to a traffic class, wherein the traffic class is defined at least in part by whether the computed second checksum should match the first checksum in the at least one packet [based on relative offsets and partial checksums (TCP/UDP protocol) calculated, other datagrams that are received with identical identification filed 333, source and destination IP addresses, are known to be another following fragment of a first fragment and subsequently added, see col. 7, lines 45-50]. The Examiner finds Bennett's process as functionally equivalent to the claimed invention.

In summary, the Applicant appears to be reading limitations from the specification into the claims, which is inappropriate. For example, "behavior pattern" is a broad term without any structural or functional limitations. The Examiner's interpretation is both reasonable and fair. Therefore, based upon the Examiner's interpretation of the claim limitations, as stated in the rejection, the claimed invention is taught.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DONALD L. MILLS whose telephone number is (571)272-3094. The examiner can normally be reached on 9:00 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chi Pham can be reached on 571-272-3179. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Donald L Mills/
Examiner, Art Unit 2416
January 17, 2009